AO 106 (Rev. 04/10) Application for a Search Warrant

UNITED STATES DISTRICT COURT

for the

Eastern District of Virginia

In the Matter of the Search of
(Briefly describe the property to be searched or identify the person by name and address)

2 HP laptops, 1 silver iPhone, 1 Black iPhone, 1 Pink iPhone, 1 Black and Sivler Alcatel One Touch phone, and 1 White Samsung Galaxy Grand Prime phone

Case No. 4:17SW29

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location)*:

See Attachment A.

located in the Eastern District of Virginia, there is now concealed *(identify the person or describe the property to be seized)*:

See Attachment B.

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☑ evidence of a crime;
- ☑ contraband, fruits of crime, or other items illegally possessed;
- ☑ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	*Offense Description*
18 U.S.C. § 1349	Conspiracy to Commit Bank Fraud
18 U.S.C. § 1344	Bank Fraud
18 U.S.C. § 1028A	Aggravated Identity Theft

The application is based on these facts:

See attached affidavit.

- ☑ Continued on the attached sheet.
- ☐ Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

REVIEWED AND APPROVED:
Kaitlin C. Gratton
Kaitlin C. Gratton
Assistant United States Attorney

Applicant's signature

Derek M. Mullins, United States Postal Inspector
Printed name and title

Sworn to before me and signed in my presence.

Date: June 9, 2017

Judge's signature

City and state: Norfolk, Virginia

The Hon. Robert J. Krask, United States Magistrate Judge
Printed name and title

AFFIDAVIT IN SUPPORT OF APPLICATION FOR SEARCH WARRANT

I, Derek Mullins, being duly sworn, hereby depose and state:

INTRODUCTION AND AGENT BACKGROUND

1. I am a Postal Inspector with the United States Postal Inspection Service ("USPIS"). I have been employed as a Postal Inspector since April 2015. Prior to becoming a Postal Inspector I was employed by the Department of Homeland Security, Immigration and Customs Enforcement ("ICE"), Homeland Security Investigations ("HSI") since August 2008. I am a graduate of the Federal Law Enforcement Training Center's Criminal Investigators Training Program and the U.S. Immigration and Customs Enforcement Academy's ICE Special Agent Training Program. Prior to my employment with HSI, I was a Deputy Sheriff with the Wise County Sheriff's Department in Wise County, Virginia from 2005 to 2008. I have received training in various aspects of federal law enforcement including the investigation of theft, fraud and narcotics related offenses as well as numerous other federal and state offenses. I have participated in multiple investigations, seizures, and search warrants which have resulted in criminal arrests, seizures, and prosecutions. I have also been the affiant on search, arrest and seizure warrants that have resulted in successful arrests, seizures, and prosecutions.

2. In the course of my employment as a sworn law enforcement officer, I have participated in the execution of search warrants resulting in the seizure of cellular telephones, computers, magnetic storage media for computers, and other items evidencing violations of state and federal laws.

REASON FOR AFFIDAVIT

3. This affidavit is made in support of an application for a warrant to search the following items, further describer in Attachment A:

RJK

DMH

a) HP Laptop, model number: 2000-410US, bearing serial number: 5CB2105VGP;

b) Silver iPhone, Model A1549; FCC ID: BCG-E2816A;

c) Black iPhone, Model A1778; FCC ID: BCG-E3091A;

d) Pink iPhone, Model A1687; FCC ID: BCG-E2944A;

e) HP Laptop, Model Notebook 15-F233WM, bearing serial number: 5CD637638G;

f) Black and Silver Alcatel One Touch cellular telephone bearing IMEI number: 014679000352893; and

g) White Samsung Galaxy Grand Prime cellular telephone bearing serial number: R28G32MMW4P.

Hereinafter collectively referred to as "Devices."

4. As set forth herein, there is probable cause to believe that the aforementioned Devices (more precisely described in Attachment A) will contain evidence, contraband, fruits or instrumentalities of violations of Title 18, United States Code, Sections 1349 (Conspiracy to Commit Bank Fraud), 1344 (Bank Fraud), and 1028A(a)(1)(Aggravated Identity Theft). Specifically, there is probable cause to believe that the items detailed in Attachment A will contain evidence of a conspiracy and scheme and artifice to defraud financial institutions and to obtain from such institutions moneys, funds, credits, assets, securities, and other property owned by and under the custody or control of such institutions by materially false and fraudulent pretenses, representations, and promises, which scheme and artifice was accomplished, at least in part, through the transfer, possession, and use of means of identifying accountholders of such institutions. In summary, conspirators used social media to identify accountholders of several financial institutions and obtain from such individuals debit cards and personal identification

RJK

DMH

numbers ("PINS") associated with accounts issued to them. Conspirators used these accounts to deposit, negotiate, and monetize worthless, counterfeit, and forged financial instruments, which conspirators deposited at automated teller machines ("ATMs") and through mobile banking Internet applications. Conspirators then used the associated debit cards and PIN numbers to conduct financial transactions, including ATM withdrawals and retail purchases of goods, services, and financial instruments, including money orders, to access the credited funds.

5. The statements contained in this affidavit are based on my training and experience, as well as information from other law enforcement officials, through interviews of witnesses, reviews of records obtained from numerous police agencies, including offense reports, arrest warrants, criminal history checks and checks of court records, and the use of other investigative techniques. Any facts and opinions cited in the affidavit, which were seen, heard, or concluded to by a law enforcement officer other than me, have been related to me by the officers who had personal knowledge thereof. All information attributed to other officers has been related to me and I believe it to be factual and truthful.

6. This affidavit is being submitted for the limited purpose of securing a search warrant. I have not included each and every fact known to me concerning this investigation. I have set forth only the facts that I believe are necessary to establish probable cause to believe that the above-referenced Devices to be searched (more precisely described in Attachment A) contain evidence, fruits and instrumentalities of violations of Title 18, United States Code, Sections 1349 (Conspiracy to Commit Bank Fraud), 1344 (Bank Fraud), and 1028A(a)(1) (Aggravated Identity Theft) (more precisely described in Attachment B).

RJC

DMA

7. The applied-for warrant would authorize the forensic examination the Devices described in Attachment A for the purpose of identifying electronically stored data particularly described in Attachment B.

RELEVANT STATUTES

8. Title 18, United States Code, Sections 1349 prohibits any person from "attempt[ing] or conspir[ing] to commit any offense under this chapter." Section 1344 is contained in the same chapter.

9. Title 18, United States Code, Sections 1344 prohibits anyone from "knowingly execut[ing], or attempt[ing] to execute, a scheme or artifice—(1) to defraud a financial institution; or (2) to obtain any of the moneys, funds, credits, assets, securities, or other property owned by, or under the custody or control of, a financial institution, by means of false or fraudulent pretenses, representations or promises."

10. Title 18, United States Code, Section 1028A prohibits anyone, during and in relation to any enumerated felony violation, from knowingly transferring, possessing, or using, without lawful authority, a means of identification of another person. Title 18, United States Code, Section 1028A enumerates felony violations, including any provision contained in chapter 63 (relating to mail, bank, and wire fraud).

DEFINITIONS

11. The term "computer," as used herein, is defined pursuant to Title 18, United States Code, Section 1030(e)(1), as "an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device."

RJK

12. The terms "records," "documents," and "materials" include all information recorded in any form, including the originals and all non-identical copies thereof, whether different from the original by reason of any notation made on such copies or otherwise, including, but not limited to the following: documents, graphic records or representations, photographs, pictures, images, spreadsheets, emails, and aural records or representations.

13. The terms "records," "documents," and "materials" include all of the foregoing, in whatever form and by whatever means, the records, documents, or materials, and their drafts, or their modifications may have been created or stored, including (but not limited to): any electrical, electronic, or magnetic form (including but not limited to any information on an electronic or magnetic storage device such as hard disks, portable storage devices or cellular phone SIM cards.

14. The "Internet" is a global network of computers and other electronic devices that communicate with each other. Due to the structure of the Internet, connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.

15. A "Universal Resource Locator" ("URL") is the unique address for a file that is accessible on the Internet. For example, a common way to get to a website is to enter the URL of the website's home page file in the Web browser's address line. Additionally, any file within that website can be specified with a URL. The URL contains the name of the protocol to be used to access the file resource, a domain name that identifies the specific computer on the Internet, and a pathname, a hierarchical description that specifies the location of a file in that computer.

16. Internet Protocol Address ("IP Address"): Every computer or device on the Internet is referenced by a unique Internet Protocol address the same way every telephone has a

RJK

unique telephone number. An example of an IP address is 192.168.10.102. Each time an individual accesses the Internet, the computer from which that individual initiates access is assigned an IP address. There are two types of IP addresses; static and dynamic. A static address is permanent and never changes, such as ones used in cable modems. The dynamic address changes almost every time the computer connects to the Internet.

17. Internet Service Providers (ISPs): Individuals who have an Internet account and an Internet-based electronic mail (e-mail) address must have a subscription, membership, or affiliation with an organization or commercial service which provides access to the Internet. A provider of Internet access and services is referred to as an Internet Service Provider or "ISP."

18. A "MAC Address" refers to the fact that every computer has a unique identifying number that is placed there by the manufacturer. It is based on a set standard on which all manufactures have agreed, and no two MAC Addresses are alike. A MAC Address is similar to the VIN number of a vehicle, as the number is not changeable.

19. "Web hosts" provide the equipment and services required to host and maintain files for one or more websites and to provide rapid Internet connections to those websites. Most hosting is "shared," which means that multiple websites of unrelated companies are on the same server in order to reduce associated costs. When a client develops a website, the client needs a server and perhaps a web hosting company to host it. "Dedicated hosting," means that the web hosting company provides all of the equipment and assumes all of the responsibility for technical support and maintenance of a website. "Co-location" means a server is located at a dedicated hosting facility designed with special resources, such as a secure cage, regulated power, a dedicated Internet connection, online security and online technical support. Co-location facilities offer customers a secure place to physically house the customers' hardware and equipment as

RJK

DMP

opposed to keeping it in their offices or warehouse, where the potential for fire, theft or vandalism is greater.

TECHNICAL TERMS

20. A "wireless telephone" (or mobile telephone, or cellular telephone) is a handheld wireless device used for voice and data communication through radio signals. These telephones send signals through networks of transmitter/receivers, enabling communication with other wireless telephones or traditional "land line" telephones. A wireless telephone usually contains a "call log," which records the telephone number, date, and time of calls made to and from the phone. In addition to enabling voice communications, wireless telephones offer a broad range of capabilities. These capabilities include: storing names and phone numbers in electronic "address books;" sending, receiving, and storing text messages and e-mail; taking, sending, receiving, and storing still photographs and moving video; storing and playing back audio files; storing dates, appointments, and other information on personal calendars; and accessing and downloading information from the Internet. Wireless telephones may also include global positioning system ("GPS") technology for determining the location of the device.

21. A "digital camera" is a camera that records pictures as digital picture files, rather than by using photographic film. Digital cameras use a variety of fixed and removable storage media to store their recorded images. Images can usually be retrieved by connecting the camera to a computer or by connecting the removable storage medium to a separate reader. Removable storage media include various types of flash memory cards or miniature hard drives. Most digital cameras also include a screen for viewing the stored images. This storage media can contain any digital data, including data unrelated to photographs or videos.

RJK

DMH

22. A "portable media player" (or "MP3 Player" or iPod) is a handheld digital storage device designed primarily to store and play audio, video, or photographic files. However, a portable media player can also store other digital data. Some portable media players can use removable storage media.

23. A "removable storage media recorder," to include a Secure Disk (SD) card and USB Flash memory drives, can store any digital data. Depending on the model, a portable media player may have the ability to store very large amounts of electronic data and may offer additional features such as a calendar, contact list, clock, or games.

24. A "GPS" navigation device uses the Global Positioning System to display its current location. It often contains records the locations where it has been. Some GPS navigation devices can give a user driving or walking directions to another location. These devices can contain records of the addresses or locations involved in such navigation. The Global Positioning System (generally abbreviated "GPS") consists of 24 NAVSTAR satellites orbiting the Earth. Each satellite contains an extremely accurate clock. Each satellite repeatedly transmits by radio a mathematical representation of the current time, combined with a special sequence of numbers. These signals are sent by radio, using specifications that are publicly available. A GPS antenna on Earth can receive those signals. When a GPS antenna receives signals from at least four satellites, a computer connected to that antenna can mathematically calculate the antenna's latitude, longitude, and sometimes altitude with a high level of precision.

25. A "personal digital assistant," or PDA, is a handheld electronic device used for storing data (such as names, addresses, appointments or notes) and utilizing computer programs. Some PDAs also function as wireless communication devices and are used to access the Internet and send and receive e-mail. PDAs usually include a memory card or other removable storage

RJK

DMA

media for storing data and a keyboard and/or touch screen for entering data. Removable storage media include various types of flash memory cards or miniature hard drives. This removable storage media can store any digital data. Most PDAs run computer software, giving them many of the same capabilities as personal computers. For example, PDA users can work with word-processing documents, spreadsheets, and presentations. PDAs may also include global positioning system ("GPS") technology for determining the location of the device.

26. Based on my training, experience, and research, and from consulting the manufacturer's advertisements and product technical specifications available online at the manufacturer websites, I know that the Devices have capabilities that allow them to serve as a wireless telephone, digital camera, portable media player, GPS navigation device, and PDA. In my training and experience, examining data stored on devices of this type can uncover, among other things, evidence that reveals or suggests who possessed or used the device. That data can also reveal with whom the possessor or user was communicating.

PROBABLE CAUSE

27. In December 2014, I became involved in an investigation into a group of individuals who were using financial institutions to negotiate fraudulent assets into cash withdrawals from ATMs. The fraud scheme began in or about August 2014 and involved the suspects soliciting current bank accountholders on social media sites, including Facebook and Instagram. At the suspects' direction and in exchange for promise of payment, the accountholders would provide their debit/credit cards and PIN numbers. The suspects would then deposit worthless or stolen checks into the compromised accounts using various ATMs in the Hampton Roads area of Virginia. Once the checks were deposited at an ATM, the bank of deposit credited the account of deposit with all or some of the check's stated value. The suspects

RJK

DMO

would then make ATM withdrawals and conduct other transactions to access the maximum allowable amount each day the account was used in the scheme. When the suspects were conducting the fraudulent withdrawals or deposits, the financial institutions had cameras recording the transactions.

28. During this investigation, Markis Jordan DICKERSON ("DICKERSON") was identified, through interviews of accountholders and debriefs of defendants, as one of the individuals conducting this scheme, alone and with others, throughout the Hampton Roads area of Virginia.

29. As part of this investigation, investigators were able to view some of DICKERSON'S publicly available activity on Facebook and Instagram. Investigators saw numerous photographs of DICKERSON holding large quantities of cash, debit/credit cards, firearms, narcotics, and ATM receipts. Investigators also identified conversations on DICKERSON'S social media accounts in which DICKERSON was soliciting accountholders for their debit/credit cards to engage in the fraud scheme. For example, investigators identified a January 2015 Facebook conversation between DICKERSON and C.W. in which DICKERSON messaged C.W. and stated, "If you got a bank account and you trynna make a couple thousand let me know." During this conversation, DICKERSON explained to C.W. how to set up a bank account and provide the "bank card" and "4 digit PIN." DICKERSON further explained that he has been able to take "official bank business checks" and "deposit 5 racks in one account."

30. In addition to these conversations, on January 22, 2015, a state search warrant was executed on an iPhone 5C bearing serial number: C7KLLA31FFHH belonging to DICKERSON. During the search of the phone, investigators located numerous photographs depicting bank receipts; debit cards; and DICKERSON posing with large sums of U.S. currency, firearms, and

RJK

DMH

narcotics. Specifically, one photograph depicted two Bayport Credit Union receipts dated December 11, 2014. Both receipts showed the last four digits of the account number. One of the receipts showed a balance of $5514.51 and the second showed a balance of $5625. Five photographs of debit cards bearing names other than DICKERSON's were identified. There was also an "account snapshot" of a Langley Federal Credit Union ("LFCU") account issued to an individual named E.B. The snapshot depicts a balance of $6,089 on December 18, 2014 and returned deposit check for -$6,084 on December 30, 2014. There was also a photograph of DICKERSON standing with a stack of U.S. currency against his ear, as if he were talking on a telephone, and holding a black handgun with an extended magazine in the other hand.

31. As a result of the 2014 investigation, four individuals were charged and convicted in the Eastern District of Virginia of conspiring to commit bank fraud, in violation of 18 U.S.C. § 1349, and aggravated identity theft, in violation of 18 U.S.C. § 1028A(a)(1). *United States v. Frazier et al.*, 4:15cr43. DICKERSON was not charged in the original investigation.

32. In approximately December 2016, I was contacted by an LFCU fraud investigator requesting assistance with an investigation that involves DICKERSON, Christopher Douglas BOONE ("BOONE"), and others concerning the use of LFCU and other financial institutions to negotiate worthless and counterfeit financial instruments into U.S. currency and other instruments. The investigator indicated that LFCU had discovered numerous transactions in multiple LFCU accounts involving the deposit of fraudulent checks and money orders and subsequent withdrawal and use of the funds credited on such deposits. LFCU had also identified purchases of money orders from retail locations through which DICKERSON, BOONE, and others obtained the cash value of the fraudulently deposited instruments. LFCU had identified

and preserved video and still surveillance images of DICKERSON, BOONE, and others conducting the transactions.

33. LFCU is a federally insured financial institution, as defined in 18 U.S.C. § 20.

34. The LFCU investigator was able to identify and interview numerous accountholders whose accounts had been used to effect the fraudulent transactions. According to the LFCU investigator, many accountholders reported that DICKERSON and others had contacted them via social media outlets to solicit their banking information. Specifically, DICKERSON and others first posted a public message seeking accountholders interested in making money. DICKERSON and others would then send private or direct messages to those who responded positively to the public message. In these private and direct messages, DICKERSON and others generally requested that all further communications be conducted via text messages or telephone calls. DICKERSON and others then directed accountholders to provide their debit cards and PINs to DICKERSON, BOONE, and others. DICKERSON and others arranged to meet accountholders at various locations to obtain debit cards and PINs, promising to deposit money into the accounts associated with such debit cards. DICKERSON, BOONE, and others then used those debit cards and PINs to effect deposits of worthless and counterfeit financial instruments, including checks and money orders, into the associated accounts. Once funds were credited to those accounts, DICKERSON, BOONE, and others used the associated debit cards and PINs to withdraw U.S. currency from ATMs and to make purchases at retail locations.

35. Debit card numbers and PINs are means of identification, as defined in 18 U.S.C. § 1028(d)(7), for the accountholders to which they are assigned.

RJK

DMA

36. As part of this investigation, I have reviewed additional postings and messages made to and through Instagram and Facebook accounts in which DICKERSON and others have discussed and attempted to further the scheme. The following are examples of such postings:

a. During the execution of a state search warrant on a Facebook account belonging to D.G., an associate of DICKERSON, investigators identified an October 31, 2016 series of direct messages between D.G. and DICKERSON concerning the scheme. DICKERSON was using the Facebook account located at http://www.facebook.com/markis.jordan.7, which was then listed under the username "Freeband Jordan." That account is currently listed under the username "Lee Swervo."

In the October 31, 2016 conversation, D.G. asked DICKERSON to explain "dat money train." DICKERSON responded, "Gotta find people wit bank accounts." D.G. stated that "presto" had been telling him/her to "get on that shit the other day navy and langly." DICKERSON responded, "Yea shit crazy we was all gettin money out here before him and Ki Ki got locked but they was droppin fake checks and sometimes it would clear but I ran into da plug himself he make the official shit on his laptop and everything it ain't no where near how we used to do it."

As a result of the 2014 investigation, I know that "presto" is a nickname used by Preston Frazier and "Ki Ki" is a nickname used by Keandre Williams. Both of these individuals were prosecuted and convicted in that investigation. *See United States v. Frazier et al.*, 4:15cr43.

b. In December 2016, investigators were monitoring DICKERSON's public Instagram account, then associated with the username "freebandkid23." Investigators observed an image posted to that account depicting an LFCU account overview, as it would appear when the account is accessed through an online banking application. The overview includes the Smart Checking and Savings accounts belonging to H.B., an accountholder investigators have associated with the current scheme. This screenshot was posted along with the following message: "Who got Langley and want 3800 in their account by tomorrow morning??"

c. In February 2017, investigators were again monitoring DICKERSON's public Instagram account. At that time, the account was associated with the user name "freebandswervo." The account appeared be the same account previously associated with the username "freebandkid23."[1] Investigators observed an image posted to that account depicting a USAA account overview, as it would appear when the account is accessed through an online banking application. The overview includes a Classic Checking account

[1] Investigators have also associated the username "bigmoney_jordan" with that same account.

RJK

DMA

belonging to H.F., another accountholder investigators have associated with the current scheme. The balance of the account was then $4,643.65. This screenshot was posted along with the following message: "Had me a good ol morning . . . HIT ME UP IF YOU WANT SOME MONEY IN YOUR ACCOUNT TODAY!!" In the days that followed this posting, investigators observed additional postings of screenshots depicting the same account with a higher available balance. One such posting showed a current balance of $12,759.24 and included the following messages: "Who want at least 4,000 in their account?" and "If you want at least 4,000 in your account DM me."

d. Also in February 2017, investigators observed an image posted to DICKERSON's public Instagram account, also made when the account was associated with the username "freebandswervo." That image depicted the same LFCU account overview for the account belonging to H.B., which investigators had previously observed in December 2016. This screenshot was re-posted along with the following message: "If you have Langley and want 3800 in your account DM me ASAP." Several Instagram users responded to the public post. DICKERSON replied on three occasions to these users advising them to contact him on his posted telephone number.

37. As part of this investigation, I have reviewed police reports filed by accountholders concerning their contact with DICKERSON and others. The following are examples of such reports:

a. According to a Newport News Police report, on or about January 6, 2017, DICKERSON contacted K.S. via social media and requested to use his/her bank account, purportedly because he was not able to access his own account. K.S. advised he/she "thought he was going to pay" him/her to use his/her bank account. They met and DICKERSON provided K.S. with two personal checks from his old account and requested he/she deposit them into his/her account. K.S. also gave DICKERSON his/her debit card and PIN. K.S. deposited the checks as requested and notified DICKERSON. K.S. was later contacted by his/her bank indicating that the checks he/she had deposited were fraudulent. K.S.'s bank further advised that additional counterfeit checks had been deposited into the account and cash withdrawals had been made at various ATMs, causing the account to be overdrawn. The bank also notified K.S. that a large purchase was made at Walmart. On January 30, 2017, Detective E. Benson met with the Asset Protection Manger at Walmart and viewed the surveillance video of the transaction described above. Detective E. Benson positively identified DICKERSON as the individual making the transaction.

b. According to a Hampton Police report, on or about January 17, 2017, DICKERSON contacted E.L. via social media and indicated that he could "make [him/her] some money." According to the police report, DICKERSON

RJK

DHH

> deposited four counterfeit checks into E.L.'s account totaling $3,853.43. After the money was deposited, DICKERSON contacted E.L. to obtain the online username and password for his/her LFCU account. DICKERSON advised he needed to login to the account and see if the money was available. DICKERSON also stated he needed to physically obtain E.L.'s debit card and PIN to ensure E.L. would "not go to the bank and steal all the money." On January 17, 2017, DICKERSON drove to E.L.'s residence and retrieved his/her debit card and PIN. On January 18, 2017, E.L. contacted LFCU and discovered that $500 had been withdrawn from the account via ATM. E.L. stated there were no funds in his/her account prior to DICKERSON depositing the counterfeit checks.

38. From approximately at least December 2016 through April 13, 2017, DICKERSON, BOONE, and others have participated in ATM transactions on more than 45 accounts issued by LFCU, SunTrust Bank ("SunTrust"), 1st Advantage Federal Credit Union ("1st Advantage"), and other financial institutions, all of which are federally insured financial institutions, as defined in 18 U.S.C. § 20. In each of these transactions, U.S. currency was withdrawn following the deposit of a worthless or counterfeit financial instrument via "remote capture deposit." A "remote capture deposit" is a deposit accomplished through the transmission of information to the institution of deposit via a mobile application on an electronic device with either cellular or internet access. During each of the withdrawals that followed such deposits, DICKERSON and BOONE were captured by ATM surveillance equipment either personally conducting the transaction or accompanying the individual(s) who conducted the transaction. Through review of LFCU's records and its interviews with actual accountholders, investigators have determined that during the period of time surrounding these transactions, the individual through whose account the transaction was done had telephonic contact with DICKERSON and/or BOONE.

39. The following are examples of the transactions identified to date as being associated with DICKERSON and BOONE:

RJK

DHM

a. On December 13, 2016, three fraudulent checks were deposited into K.M.'s LFCU account via remote capture deposit. On the same day, four transactions were attempted/conducted at an LFCU branch located on West Mercury Boulevard in Hampton, Virginia. The first transaction was an attempted ATM withdrawal at the drive-thru ATM using K.M.'s debit card and PIN. BOONE was captured by the ATM's surveillance equipment driving a black car through the drive-thru ATM and attempting to withdraw $500 from K.M's account at that ATM. After the transaction was declined, BOONE then attempted a second successful withdraw of $300 from K.M.'s account. DICKERSON was captured by the ATM's surveillance equipment in the passenger seat beside BOONE during these transactions. Approximately two minutes after BOONE drove away from the ATM, DICKERSON was captured by the walk-up ATM's surveillance equipment conducting two separate withdrawals; each for $100. K.M.'s debit card and PIN were used during each of these transactions.

b. On January 26, 2017, three counterfeit checks were deposited into J.B.'s LFCU account via remote capture deposit. That same day, BOONE was captured by ATM surveillance equipment using J.B.'s debit card and PIN to withdraw $500 from J.B.'s account at the drive-thru LFCU ATM located on West Mercury Boulevard in Hampton, Virginia. On January 29, 2017, one counterfeit check was deposited into J.B.'s account via remote capture deposit. On January 30, 2017, one counterfeit check was deposited into J.B.'s account via remote capture deposit. That same day, DICKERSON was captured by ATM surveillance equipment using J.B.'s debit card and PIN to withdraw $500 from J.B.'s account at the walk-up ATM at the same LFCU branch located on West Mercury Boulevard in Hampton, Virginia.

40. On March 1, 2017, DICKERSON and BOONE were arrested by the Newport News Police Department, Hampton Police Division, and the United States Postal Inspection Service during a traffic stop in Hampton, Virginia. On that date, DICKERSON was observed driving a 2009 Mercedes Benz, white in color, registered to DICKERSON through the Virginia Department of Motor Vehicles, with two other occupants. BOONE was identified as the sole rear-seat passenger, located immediately behind the driver. At the time of his arrest, DICKERSON was found with a stolen handgun loaded with a high-capacity magazine concealed in his waist band. Incident to arrest, the vehicle was searched for weapons immediately accessible to DICKERSON or the other passengers in the vehicle. A second handgun was found

under the driver's seat, immediately accessible to BOONE. Inspection of the driver's seat revealed that the area from which this second handgun was recovered was not accessible from the driver's seat, only from the rear passenger seat, as a result of the motorized seat components. During the weapons sweep of the vehicle, investigators also observed credit/debit cards bearing names of individuals who were not in the vehicle. At that time, investigators stopped the search, maintained control of the vehicle, and applied for a state search warrant.

41. That same day, investigators executed a state issued search warrant on the vehicle described above. During the search, investigators located more credit/debit cards bearing names of individuals who were not in the vehicle; two counterfeit checks bearing the City of Norfolk seal and the name of a known accountholder; an HP laptop computer, model number 2000-410US; a printer; and numerous pages of blank check stock. Investigators also seized three cellular telephones: a black iPhone, Model A1778; and a pink iPhone, Model A1687; and a silver iPhone, Model A1549. The black and pink iPhones belonged to BOONE and the silver iPhone belonged to DICKERSON. The electronic items recovered during this search are further described in Attachment A.

42. Based on information gathered from the investigation, investigators applied for and were issued a state search warrant for BOONE's residence located on Friendly Drive, in Hampton, Virginia. Investigators executed the search warrant on BOONE's residence on March 1, 2017. Inside the residence, investigators located and seized, among other items, two printers, an HP laptop computer, model Notebook 15-F233WM, hundreds of pages of blank check stock, numerous credit/debit cards in various names, counterfeit checks bearing the City of Norfolk seal and the name of the same known accountholder printed on the counterfeit checks found in DICKERSON's vehicle.

43. All of the items that were seized during the execution of the warrants on March 1, 2017 were packaged and placed into evidence at the Hampton Police Department. On April 27, 2017, these items were transferred to the United States Postal Inspection Service and placed into evidence, where they remain.

44. Based on the information obtained from the investigation and evidence recovered during the execution of the above-described warrants, BOONE and DICKERSON were both charged in Hampton, Virginia with 18.2-178 (Obtaining Money by False Pretense). BOONE was also charged with 18.2-308.2 (Possession of a Firearm by a Convicted Felon).

45. BOONE remained in stated custody after after his arrest on March 1, 2017.

46. On March 9, 2017, DICKERSON was issued a bond in the Hampton, Virginia Court. DICKERSON posted bond later the same evening and was released from the Hampton, Virginia jail.

47. After his release, DICKERSON was identified in ATM surveillance images conducting additional transactions to access funds credited to accounts following remote capture deposits of worthless and counterfeit checks, including but not limited to the following transactions:

a. On April 5, 2017, a counterfeit check was deposited into A.O.'s LFCU account via remote capture deposit. That same day, DICKERSON was captured by ATM surveillance equipment using A.O.'s debit card and PIN attempting to withdraw $500 from A.O.'s account at a walk-up ATM located on Jefferson Avenue in Newport News, Virginia.

b. On April 12, 2017, DICKERSON was captured by ATM surveillance equipment depositing an altered Western Union money order into D.G.'s 1st Advantage Bank account. That same day, DICKERSON was again captured by ATM surveillance equipment using D.G.'s debit card and PIN as he withdrew $100 from D.G.'s account at the drive-through ATM located at the 1st Advantage Bank on West Mercury Boulevard in Hampton, Virginia.

RJK

DMA

48. On April 12, 2017, a federal grand jury sitting in Newport News returned a 17-count indictment charging DICKERSON and BOONE with conspiring to commit bank fraud, in violation of 18 U.S.C. § 1349 (Count 1); bank fraud, in violation of 18 U.S.C. § 1344 (Counts 2-9); and aggravated identity theft, in violation of 18 U.S.C. § 1028A(a)(1) (Counts 10-16). The indictment also charged BOONE with possessing a firearm as a convicted felon, in violation of 18 U.S.C. § 922(g)(1) (Count 17).

49. On April 13, 2017, DICKERSON was pulled over in a traffic stop in Hampton, Virginia. On that occasion, DICKERSON was driving the same vehicle he had been operating on March 1, 2017. During the stop, DICKERSON was arrested on the outstanding federal arrest warrant. Incident to arrest, officers from the Hampton Police Division located on DICKERSON's person a black and silver Alcatel One Touch cellular telephone, further described in Attachment A. After arresting DICKERSON, officers conducted an inventory of DICKERSON's 2009 Mercedes Benz prior to having it towed. During the inventory, officers located several debit cards within the passenger compartment, immediately accessible to the driver's seat. Two of the debit cards were in the names A.O. and D.G., accountholders whose accounts DICKERSON accessed after he was released on bond, as described above. Officers also located in the passenger compartment a white Samsung Galaxy Grand Prime cellular telephone, further described in Attachment A, as well as a printer and blank check stock.

50. All of the items that were recovered from the inventory of DICKERSON's vehicle were turned over to Newport News Police Detective and U.S. Postal Inspection Service Task Force Officer (TFO) E. Benson. These items were entered into to Newport News Property and Evidence, where they currently remain.

RJK

DLM

51. DICKERSON made his initial appearance on April 14, 2017. Boone made his initial appearance on June 2, 2017. Trial is currently set for September 6, 2017.

USE OF COMPUTERS, CELLULAR TELEPHONES, AND OTHER ELECTRONIC DEVICES

52. Based on my training and experience, as well as information obtained from this investigation, I know that computers and other electronic devices, such as those described in Attachment A, also have the ability to access the Internet through the use of a Wi-Fi connection. The Wi-Fi connection is utilized wirelessly without the aid of a telephone line and operates via radio waves over a computer network attached to an internet service provider. Information can be sent and received in the same manner as if the device is attached to the local network via telephone or high speed broadband to the internet service provider.

53. I know that devices capable of accessing the internet are assigned Internet Protocol Addresses (IP Addresses), which are often specific to the individual device. I also know that these IP Addresses are often captured and maintained by sites accessed through mobile applications, including social media sites and banks.

54. Computer hardware, software, electronic files, portable storage devices, and GPS devices may be important to a criminal investigation in two distinct ways: (1) the objects themselves may be contraband, evidence, instrumentalities, or fruits of crime, and/or (2) the objects may be used as storage devices that contain contraband, evidence, instrumentalities, or fruits of crime in the form of electronic data. Rule 41 of the Federal Rules of Criminal Procedure permits the government to search for and seize computer hardware, software, and electronic files, portable storage devices, GPS and cellular telephones that are evidence of crime, contraband, instrumentalities of crime, and/or fruits of crime.

RJK

DHW

55. Based on my training and experience, as well as information obtained from this investigation, I know that computers and other electronic devices, such as those described in Attachment A, are capable of downloading and accessing programs that can be used to create or alter documents, to include personal and business checks. Computers and computer programs are often used in the production of counterfeit checks. I know that when computers are found in close proximity to blank check stock and printed counterfeit checks, as is the case here, it is more likely that those computers and their programs have been used for that purpose.

56. I know that computers and computers are also capable of storing images and documents that are created and/or modified for future use. The computer's capability to store images in digital form makes it an ideal repository for bank fraud and identity theft. The size of the electronic storage media (commonly referred to as a hard drive) used in home computers has grown tremendously within the last several years. Hard drives with the capacity of sixty (60) to two hundred (200) gigabytes are not uncommon. These drives can store thousands of images at very high resolution. Magnetic storage located in host computers adds another dimension to the equation. It is possible to use a video camera to capture an image, process that image in a computer with a video capture board, and save that image to storage in another country. Once this is done, there is no readily apparent evidence at the scene of the crime. Only with careful laboratory examination of electronic storage devices is it possible to recreate the evidence trail.

57. Based on my training and experience, as well as information obtained from this investigation, I know that cellular phones, such as those described in Attachment A, have many of the same characteristics as computers. They act as portable storage devices that can be used to capture and transport vast amounts of data from computers to cell phones and vice versa. This is particularly true for smart phones, such as iPhones, Android and Motorola phones, which have

RJK

DMA

the ability to access multiple applications, including email and the internet. Among other things, I also know that such phones are capable of downloading and accessing mobile applications, including applications that allow a user to access social mediate sites, including Facebook and Instagram, as well as mobile banking applications that allow users to conduct remote capture deposits. Many of these applications are capable of temporarily storing images uploaded or transmitted through such applications.

58. Like computers, cellular phones like those described in Attachment A knows may be important to a criminal investigation in two distinct ways: (1) the objects themselves may be contraband, evidence, instrumentalities, or fruits of crime, and/or (2) the objects may be used as storage devices that contain contraband, evidence, instrumentalities, or fruits of crime in the form of electronic data. Rule 41 of the Federal Rules of Criminal Procedure permits the government to search for and seize cellular telephones that are evidence of crime, contraband, instrumentalities of crime, and/or fruits of crime.

59. Based on my training and experience, subjects involved in criminal activity regularly use cellular telephones and cellular telephones' features i.e., text-messaging, photos, etc., to communicate with other parties involved in criminal activity. I know that cellular telephones are capable of sending electronic communications such as text messages, iMessages, emails, and other forms of electronic communication. I know these devices are capable of storing these messages for an extended period of time. I also know that individuals who use cellular telephones and other electronic devices often maintain a "contact list," or list of names and numbers of individuals with whom they often communicate. It is my belief that a search of the cellular telephones listed in Attachment A will show communications between the suspects and may identify other co-conspirators or accountholders.

60. Based on my training and experience, I know that cellular phones are capable of being used to send and receive text messages, photographs, short videos, other electronic data and voice communication. I know that cellular phones contain internal memory, which can store records of received, dialed, and missed calls on that particular phone. That cellular phone memory also stores downloaded ring tones, data downloaded from the internet, pictures, text messages, phone books, date books, address books, and other data. Many users will program the phone with personal information to identify the owner of that particular phone. The phone will always store the last number dialed, along with information about the geographical location of the cellular tower that was used to place the last phone call.

61. As outlined, herein, there is probable cause to believe that the cellular phones, referenced in Attachment A, contain evidence of the crimes of conspiracy to commit bank fraud, bank fraud, and aggravated identity theft, in that based on my training and experience and the evidence developed thus far in the investigation, DICKERSON and BOONE used mobile applications to access social media and banking sites and to communicate with accountholders.

62. I expect the cellular telephones to maintain the number of the phone, a list of telephone numbers and name of the user of said telephone number stored in the phonebook of the phone, a record of the most recent outgoing calls, incoming calls, and missed calls, voicemail messages, email messages, text messages, voice recordings, stored memos and calendars, still photographic images, video photographic images and any other stored electronic information. It is respectfully requested that the search warrant sought by this application authorize a full physical and forensic examination of the cellular phones, including their SIM cards, referenced in Attachment A.

RJK

DKW

SPECIFICS OF THE SEARCH OF COMPUTERS

63. Computer hardware consists of all equipment, which can collect, analyze, create, display, convert, store, conceal, or transmit electronic, magnetic, optical, or similar computer impulses or data. Hardware includes (but is not limited to) any data-processing devices (such as central processing units, memory typewriters, and self-contained "lap-top" or "notebook" computers); internal and peripheral storage devices (such as fixed disks, external hard disks, floppy disk drives and diskettes, tape drives and tapes, optical storage devices, transistor-like binary devices and other memory storage devices); peripheral input/output devices (such as keyboards, printers, scanners, plotters, video display monitors, and optical readers); and related communications devices (such as modems, cables and connections, recording equipment, RAM, or ROM units, acoustic couplers, automatic dialers, speed dialers, programmable telephone dialing or signaling devices, and electronic tone-generating devices); as well as any devices, mechanisms, or parts that can be used to restrict access to computer hardware (such as physical keys and locks).

64. Computer software is digital information, which can be interpreted by a computer and any of its related components to direct the way they work. Software is stored in electronic, magnetic, optical, or other digital form. It commonly includes programs to run operating systems, applications (like word-processing, graphics, or spreadsheet programs), utilities, compilers, interpreters, and communications programs.

65. Computer-related documentation consists of written, recorded, printed, or electronically stored material, which explains or illustrates how to configure or use computer hardware, software, or other related items.

66. Computer passwords and other data security devices are designed to restrict access to or hide computer software, documentation, or data. Data security devices may consist of hardware, software, or other programming code. A password (a string of alpha-numeric characters) usually operates as a sort of digital key to "unlock" particular data security devices. Data security hardware may include encryption devices, chips, and circuit boards. Data security software or digital code may include programming code that creates "test" keys or "hot" keys, which perform certain pre-set security functions when touched. Data security software or code may also encrypt, compress, hide, or "booby-trap" protected data to make it inaccessible or unusable, as well as reverse the process to restore it.

67. Based on my knowledge, training, and experience, I know that searching and seizing information from computers and cellular phones, such as those described in Attachment A, often requires agents to seize most or all electronic storage devices (along with related peripherals) to be searched later by a qualified computer expert in a laboratory or other controlled environment. This is true because of the following:

a. The volume of evidence. Computer storage devices (like hard disks, diskettes, tapes, laser disks, Bernoulli drives), including smart phone devices such as iPhones, Android, and Motorola phones, which are computer based, can store the equivalent of thousands of pages of information. Additionally, a suspect may try to conceal criminal evidence; he or she might store it in random order with deceptive name files. This may require searching authorities to examine all the stored data to determine which particular files is evidence or instrumentalities of crime. This sorting process can take weeks or months, depending on the volume of data stored, and it would be impractical to attempt this kind of data search on site.

b. Technical requirements. Searching computer systems and smart phone devices for criminal evidence is a highly technical process requiring expert skill and a properly controlled environment. The vast array of computer hardware and software available requires even computer experts to specialize in some systems and applications, so it is difficult to know before a search which expert is qualified to analyze the system and its data. In any event, however, data search protocols are exacting scientific procedures designed to protect the integrity of the evidence and to recover even "hidden," erased, compressed, password-

RJK

DMC

protected, or encrypted files. Since computer evidence is extremely vulnerable to inadvertent or intentional modification or destruction (both from external sources or from destructive code imbedded in the system as a "booby trap"), a controlled environment is essential to its complete and accurate analysis.

c. The peripheral devices, which allow users to enter or retrieve data from the storage devices, vary widely in their compatibility with other hardware and software. Many system storage devices require particular input/output (or "I/O") devices in order to read the data on the system. It is important that the analyst be able to properly reconfigure the system as it now operates in order to accurately retrieve the evidence listed above. In addition, the analyst needs the relevant system software (operating systems, interfaces, and hardware drivers) and any applications software, which may have been used to create the data (whether stored on hard drives or on external media), as well as all related instruction manuals or other documentation and data security devices.

d. Data analysts may use several different techniques to search electronic data for evidence or instrumentalities of crime. These include, but are not limited to the following: examining file directories and subdirectories for the lists of files they contain; "opening" or reading the first few "pages" of selected files to determine their contents; scanning for deleted or hidden data; searching for key words or phrases ("string searches").

68. Based on my knowledge, training, and experience, I know that documents and pictures that are scanned as a digital image are often stored permanently as a file on the host computer's hard drive. I know that even in the event a user attempts to erase such files from his or her computer system, it is possible to forensically recover such files/images long after they have been erased.

SPECIFICS OF THE SEARCH OF CELLULAR PHONES

69. Based on my training and experience, I know that a cellular phone is capable of storing photographs, electronic data including websites and contact information. I also know that a smart phone contains internal memory, which can store internet protocol address (IP) information that identify the website the owner has accessed and used the device along with the IP addresses that the device has accessed.

70. I also knows that cellular phones are equipped with Subscriber Identity Module (SIM) cards. A SIM card is a removable chip inside a cellular phone that contains information such as the user's phone number, phone book, as well as other information related to the subscriber.

71. Based on my training and experience, I know that a cellular phone is capable of storing photographs and electronic data, including websites and contact information. I also know that a smart phone contains internal memory, which can store internet protocol address (IP) information that identifies the websites the owner has accessed and used on the device, along with the IP addresses that the device has accessed.

72. I also know that a forensic examination may be performed on a cellular phone and the SIM card to retrieve information as well as on the internal memory of a smart phone. Cellular phones save and delete information on both the internal memory and SIM card and even though an item may have been deleted it is still possible to recover the deleted files. It takes specialized training and experience along with software and hardware to perform a forensic examination and analysis of a cellular phone to retrieve this information. A forensic examiner may be able to recover evidence such as photographs, text messages, videos, phone books, call history and the geographical location of the cellular phone during certain phone calls by doing a forensic examination.

ELECTRONIC STORAGE AND FORENSIC ANALYSIS

73. Based on my knowledge, training, and experience, I know that electronic devices can store information for long periods of time. Similarly, things that have been viewed via the Internet are typically stored for some period of time on the device. This information can sometimes be recovered with forensics tools.

74. *Forensic evidence.* As further described in Attachment B, this application seeks permission to locate not only electronically stored information that might serve as direct evidence of the crimes described on the warrant, but also forensic evidence that establishes how the Device was used, the purpose of its use, who used it, and when. There is probable cause to believe that this forensic electronic evidence might be on the Device because:

e. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file).

f. Forensic evidence on a device can also indicate who has used or controlled the device. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence.

g. A person with appropriate familiarity with how an electronic device works may, after examining this forensic evidence in its proper context, be able to draw conclusions about how electronic devices were used, the purpose of their use, who used them, and when.

h. The process of identifying the exact electronically stored information on a storage medium that are necessary to draw an accurate conclusion is a dynamic process. Electronic evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

i. Further, in finding evidence of how a device was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium.

75. *Nature of examination.* Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit the examination of the devices consistent with the warrant. The examination may require authorities to employ techniques, including but not limited to computer-assisted scans of the entire medium, that might expose

many parts of the devices to human inspection in order to determine whether they are evidence described by the warrant.

76. *Manner of execution.* Because this warrant seeks only permission to examine devices already in law enforcement's possession, the execution of this warrant does not involve the physical intrusion onto a premises. Consequently, I submit there is reasonable cause for the Court to authorize execution of the warrant at any time in the day or night.

CONCLUSION

77. Based on the information set forth in this affidavit, I respectfully submit there is probable cause to believe, that on the items further described in Attachment A, there is now evidence, fruits, and instrumentalities of violations of Title 18, United States Code, Sections 1349 (Conspiracy to Commit Bank and Wire Fraud), 1344 (Bank Fraud), and 1028A(a)(1) (Aggravated Identity Theft). Furthermore, there is probable cause to believe, that on the Devices further described in Attachment A, there is now information that will assist law enforcement to identify further crimes, co-conspirators, and victims that may not be currently known by law enforcement.

78. Based on my training and experience, and the facts set forth in this affidavit, I respectfully submit that this affidavit supports probable cause for a search warrant authorizing the examination of the Devices further described in Attachment A, pursuant to Rule 41 of the Federal Rules of Criminal Procedure, to seek the items described in Attachment B.

Respectfully submitted,

D.M. Mullins, U.S. Postal Inspector
United States Postal Inspection Service
Richmond, Virginia

Reviewed for legal sufficiency by:

Kaitlin C. Gratton

Kaitlin C. Gratton
Assistant United States Attorney

Subscribed and sworn before me this 9th day of June, 2017 at ~~Newport News,~~ Norfolk, Virginia.

Robert J. Krask

UNITED STATES MAGISTRATE JUDGE

RJK

ATTACHMENT A

DESCRIPTION OF ITEMS TO BE SEARCHED

All items listed below, which are currently held in the U.S. Postal Inspection Service Evidence in Richmond, Virginia:

a) HP Laptop, Model number: 2000-410US, bearing serial number: 5CB2105VGP, recovered from trunk of Mercedes recovered on 3/1/2017;

b) Silver iPhone, Model A1549; FCC ID: BCG -E2816A, recovered from front passenger compartment of Mercedes on 3/1/2017;

c) Black iPhone, Model A1778; FCC ID: BCG -E3091A; recovered from rear passenger compartment of Mercedes on 3/1/2017;

d) Pink iPhone, Model A1687; FCC ID: BCG -E2944A; recovered from rear passenger compartment of Mercedes on 3/1/2017;

e) HP Laptop, Model Notebook 15-F233WM, bearing serial number: 5CD637638G; recovered from kitchen area of BOONE's Hampton, Virginia residence on 3/1/2017;

f) Black and Silver Alcatel One Touch cellular telephone bearing IMEI number 014679000352893; recovered from DICKERSON's person on 4/13/2017; and

g) White Samsung Galaxy Grand Prime cellular telephone bearing serial number R28G32MMW4P; recovered from front passenger compartment of Mercedes on 4/13/2017.

ATTACHMENT B

PARTICULAR THINGS TO BE SEIZED

Evidence of violations of Title 18, United States Code, Section 1349 (Conspiracy to Commit Bank Fraud); 1344 (Bank Fraud); and Title 18, United States Code, Section 1028A (Aggravated Identity Theft), which may be found in the items listed in Attachment A, including:

a. Electronically stored data, files, or digital information including records, documents, materials, images, photographs, files, notes, emails, electronic communications, ISP addresses, and account information relating to the above-referenced violations;

b. Computer system information and file structure data;

c. Any documents, records, programs, or applications that identify the owner of the subject device;

d. Any documents, records, programs or applications that could be used to create, alter, reproduce, or print checks or other financial documents or accounts, and any stored data, files, digital information, records, documents, materials, images, files, and notes showing use of such documents, records, programs, or applications to create, alter, reproduce, or print checks or other financial documents or accounts;

e. Any personal identifying information belonging to any victim or accountholder or other person not involved in the conspiracy;

f. Any electronically stored communications or messages pertaining to the above-referenced violations that are maintained on the subject device or that have been deleted from the device but may be recoverable, including communications among co-conspirators and accountholders;

g. Any notes, images, photographs, emails, and electronic communications containing debit cards, debit card numbers, accountholder information, and PINs;

h Any Geo Positioning System (GPS) location or coordinate(s), directions, or maps saved or deleted from the subject device pertaining to the above-referenced violations;

i. Any documents, records, programs or applications that identify the Internet service provided to the subject device or the Internet Protocol Address (IP Address) of the subject device;

j. Any photographs depicting persons, places, or items relating to the above-referenced violations;

RJK
DMA

k. Any records, files, cookies, or other information contained identifying websites visited and Internet searches and browsing history;

l. Any documents, records, programs, or applications that can be used to access social media sites, including Facebook and Instagram, and online and mobile banking sites, including sites that can be used to make remote capture deposits; and any stored data, files, digital information, records, documents, materials, images, files, and notes showing use of these applications, including stored login information, passwords, and dates and times on which such applications were accessed and used; and.

m. Deleted, altered, damaged, or corrupted data stored in the same areas or relating to the same violations stated above.